Anni *et al. Research in Number Theory* (2016) 2:1
DOI 10.1007/s40993-015-0032-4

Research in Number Theory
a SpringerOpen Journal

RESEARCH Open Access

Residual representations of semistable principally polarized abelian varieties

Samuele Anni*, Pedro Lemos and Samir Siksek

*Correspondence:
samuele.anni@gmail.com
Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom

Abstract

Let $A/\mathbb{Q}$ be a semistable principally polarized abelian variety of dimension $d \geq 1$. Let ℓ be a prime and let $\overline{\rho}_{A,\ell}\colon G_{\mathbb{Q}} \to \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ be the representation giving the action of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-torsion group $A[\ell]$. We show that if $\ell \geq \max(5, d+2)$, and if image of $\overline{\rho}_{A,\ell}$ contains a transvection then $\overline{\rho}_{A,\ell}$ is either reducible or surjective. With the help of this we study surjectivity of $\overline{\rho}_{A,\ell}$ for semistable polarized abelian threefolds, and give an example of a genus 3 hyperelliptic curve $C/\mathbb{Q}$ such that $\overline{\rho}_{J,\ell}$ is surjective for all primes $\ell \geq 3$, where J is the Jacobian of C.

Keywords: Galois representations, Abelian varieties, Semistability, Serre's uniformity

2010 Mathematics Subject Classification: Primary 11F80, Secondary 11G10, 11G30

1 Background

Let A be a principally polarized abelian variety of dimension d defined over $\mathbb{Q}$. Let ℓ be a prime and write $A[\ell]$ for the ℓ-torsion subgroup of $A(\overline{\mathbb{Q}})$. This is a $2d$-dimensional $\mathbb{F}_\ell$-vector space, as well as a $G_{\mathbb{Q}}$-module, where $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The polarization induces the mod ℓ Weil pairing on $A[\ell]$, which is a bilinear, alternating, non-degenerate pairing

$$\langle\,,\,\rangle : A[\ell] \times A[\ell] \to \mathbb{F}_\ell(1)$$

that is Galois equivariant. The latter property means $\langle \sigma v, \sigma v' \rangle = \chi(\sigma)\langle v, v' \rangle$ for all $\sigma \in G_{\mathbb{Q}}$, and $v, v' \in A[\ell]$ where $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ is the mod ℓ cyclotomic character. In particular, the space $(A[\ell], \langle\,,\,\rangle)$ is a symplectic $\mathbb{F}_\ell$-vector space of dimension $2d$. We obtain a representation

$$\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}(A[\ell], \langle\,,\,\rangle) \cong \mathrm{GSp}_{2d}(\mathbb{F}_\ell).$$

The study of images of representations $\overline{\rho}_{A,\ell}$ has received much attention recently (e.g. [1, 4, 5]). This study is largely motivated by the following remarkable result of Serre.

Theorem 1 (Serre, [12] Theorem 3). *Let A be a principally polarized abelian variety of dimension d, defined over $\mathbb{Q}$. Assume that $d = 2$, 6 or d is odd and furthermore assume that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Then there exists a bound B_A such that for all primes $\ell > B_A$ the representation $\overline{\rho}_{A,\ell}$ is surjective.*

For explicit (though large) estimates for the constant B_A see [7]. The conclusion of the theorem is known to be false for general d; a counterexample is constructed by Mumford

[9] for $d = 4$. The following is a tantalizing open question: *given d as in the theorem, is there a uniform bound B_d depending only on d, such that for all principally polarized abelian varieties A over $\mathbb{Q}$ of dimension d with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$, and all $\ell > B_d$, the representation $\overline{\rho}_{A,\ell}$ is surjective?* For elliptic curves an affirmative answer is expected, and this is known as Serre's Uniformity Question, which is still an open problem. Serre's Uniformity Question is much easier for semistable elliptic curves. Indeed, Serre ([11], Proposition 21) shows that if $E/\mathbb{Q}$ is a semistable elliptic curve, and $\ell \geq 7$ is prime, then $\overline{\rho}_{E,\ell}$ is either surjective or reducible. It immediately follows from Mazur's classification [8] of isogenies of elliptic curves over $\mathbb{Q}$ that $\overline{\rho}_{E,\ell}$ is surjective for $\ell \geq 11$. It is natural to ask if a result similar to Serre's ([11], Proposition 21) can be established for semistable principally polarized abelian varieties. For now, efforts to prove such a theorem are hampered by the absence of a satisfactory classification of maximal subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ (indeed, Serre's result for semistable elliptic curves makes use of Dickson's classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell) = \mathrm{GSp}_2(\mathbb{F}_\ell)$). There is however a beautiful classification due to Arias-de-Reyna, Dieulefait and Wiese (see Theorem 3 below) of subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ containing a transvection. A *transvection* is a unipotent element σ such $\sigma - I$ has rank 1. The main result of our paper, building on the classification of Arias-de-Reyna, Dieulefait and Wiese, is the following theorem.

Theorem 2. *Let A be a semistable principally polarized abelian variety of dimension $d \geq 1$ over $\mathbb{Q}$ and let $\ell \geq \max(5, d+2)$ be prime. Suppose the image of $\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ contains a transvection. Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.*

The proof of Theorem 2 is given in Section 2. We mention a well-known pair of sufficient conditions (see for example [5], Section 2) for the image of $\overline{\rho}_{A,\ell}$ to contain a transvection. Let $q \neq \ell$ be a prime and suppose that the following two conditions are satisfied:

- The special fibre of the Néron model for A at q has toric dimension 1;
- $\ell \nmid \#\Phi_q$, where Φ_q is the group of connected components of the special fibre of the Néron model at q.

Then the image of $\overline{\rho}_{A,\ell}$ contains a transvection. Now let $C/\mathbb{Q}$ be a hyperelliptic curve of genus d, given by a model $y^2 = f(x)$ where $f \in \mathbb{Z}[x]$ is a squarefree polynomial. Let p be an odd prime not dividing the leading coefficient of f such that f modulo p has one root in $\overline{\mathbb{F}}_p$ having multiplicity precisely 2, with all other roots simple. Then the Néron model for the Jacobian $J(C)$ (which is a principally polarized abelian variety) at p has toric dimension 1.

The remainder of the paper is concerned with semistable principally polarized abelian threefolds $A/\mathbb{Q}$ which possess a prime q such that the special fibre of the Néron model for A at q has toric dimension 1. Building on Theorem 2, we give in Section 3 a practical method which should in most cases produce an explicit (and small) bound B (depending on A) such that for $\ell \geq B$, the representation $\overline{\rho}_{A,\ell}$ is surjective. This method is inspired by the paper of Dieulefait [4] which solves the corresponding problem for abelian surfaces. Our method is not always guaranteed to succeed, but we expect it to succeed if $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$.

It is well known that $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ is a Galois group over $\mathbb{Q}$ for all $d \geq 1$ and all primes $\ell \geq 3$ (see for example [1], Remark 2.5). The proof of this statement in fact shows the

existence of a genus d hyperelliptic curve $C/\mathbb{Q}$ such that $\overline{\rho}_{J,\ell}$ is surjective, where J is the Jacobian of C. The argument however relies on Hilbert's Irreducibility Theorem, and so does not produce an explicit equation for C. In [1], a genus 3 hyperelliptic curve $C/\mathbb{Q}$ is given so that $\overline{\rho}_{J,\ell}$ is surjective for all $11 \leq \ell < 5 \times 10^5$. As a corollary to our method for producing the bound B mentioned above, we prove the following.

Corollary 1.1. *Let $C/\mathbb{Q}$ be the following genus 3 hyperelliptic curve,*

$$C \,:\, y^2 + \left(x^4 + x^3 + x + 1\right) y = x^6 + x^5. \tag{1}$$

and write J for its Jacobian. Let $\ell \geq 3$ be a prime. Then $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_\ell)$.

Recently (and independently), Zywina [13] gives a genus 3 plane quartic curve over $\mathbb{Q}$ for which he proves that the Galois action on the torsion subgroup of the Jacobian J is maximal (in other words, $\rho_J \colon G_{\mathbb{Q}} \to \mathrm{GSp}_6\left(\hat{\mathbb{Z}}\right)$ is surjective).

We are grateful to Tim Dokchitser for providing us with a list of genus 3 hyperelliptic curves with small Jacobian conductors, from which we chose the curve C in Corollary 1.1. We thank Jeroen Sijsling for helpful remarks on an earlier version of this paper. We are indebted to the referees for their careful reading of the paper and for many helpful remarks.

2 Proof of Theorem 2

We shall make use of the following classification of subgroups of $\mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ containing a transvection, due to Arias-de-Reyna, Dieulefait and Wiese.

Theorem 3 (Arias-de-Reyna, Dieulefait and Wiese, [2])**.** *Let $\ell \geq 5$ be a prime and let V a symplectic $\mathbb{F}_\ell$-vector space of dimension $2d$. Any subgroup G of $\mathrm{GSp}(V)$ which contains a transvection satisfies one of the following assertions:*

- *(i)* *There is a non-trivial proper G-stable subspace $W \subset V$.*
- *(ii)* *There are non-singular symplectic subspaces $V_i \subset V$ with $i = 1, \ldots, h$, of dimension $2m < 2d$ and a homomorphism $\phi \,:\, G \to S_h$ such that $V = \oplus_{i=1}^{h} V_i$ and $\sigma(V_i) = V_{\phi(\sigma)(i)}$ for $\sigma \in G$ and $1 \leq i \leq h$. Moreover, $\phi(G)$ is a transitive subgroup of S_h.*
- *(iii)* $\mathrm{Sp}(V) \subseteq G$.

We shall apply Theorem 3 to $G = \overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ where A and ℓ are as in the statement of Theorem 2. It follows from the surjectivity of the mod ℓ cyclotomic character $\chi \colon G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ that if $\mathrm{Sp}_{2d}(\mathbb{F}_\ell) \subseteq G$ then $G = \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$.

Throughout we write I_ℓ for the inertia at ℓ subgroup of $G_{\mathbb{Q}}$. We shall also make use of the following theorem of Raynaud.

Theorem 4 (Raynaud, [10])**.** *Let A be an abelian variety over $\mathbb{Q}$. Let ℓ be a prime of semistable reduction for A. Regard $A[\ell]$ as an I_ℓ-module and let V be a Jordan-Hölder factor of dimension n over $\mathbb{F}_\ell$. Let $\psi_n \,:\, I_\ell \to \mathbb{F}_{\ell^n}^\times$ be a fundamental character of level n. Then V has the structure of a 1-dimensional $\mathbb{F}_{\ell^n}$-vector space and the action of I_ℓ on it is given by a character $\varpi \,:\, I_\ell \to \mathbb{F}_{\ell^n}^\times$, where $\varpi = \psi_n^{\sum_{i=0}^{n-1} a_i \ell^i}$ with $a_i = 0$ or 1.*

We shall make use of the following elementary lemma in the proof of Theorem 2.

Lemma 2.1. *Let k be an algebraically closed field and $V \neq 0$ be a finite dimensional vector space over k. Let $T\colon V \to V$ be a k-linear map, and suppose $V = \oplus_{i=1}^{r} V_i$ where $T(V_i) = V_{i+1}$ (the indices considered modulo r). Let α be an eigenvalue of T. Then $\zeta\alpha$ is also an eigenvalue of T for every ζ in k satisfying $\zeta^r = 1$.*

Proof. Let v be an eigenvector corresponding to α and write $v = \sum_{i=1}^{r} v_i$ with $v_i \in V_i$. Then $T(v_i) = \alpha v_{i+1}$. Let $v' = \sum_{i=1}^{r} \zeta^{-i} v_i$. Then $T(v') = \sum_{i=1}^{r} \zeta^{-i}\alpha v_{i+1} = \zeta\alpha \sum_{i=1}^{r} \zeta^{-i-1} v_{i+1} = \zeta\alpha v'$ showing that $\zeta\alpha$ is indeed an eigenvalue. □

Proof of Theorem 2. Denote $\overline{\rho} = \overline{\rho}_{A,\ell}$. Let $G = \overline{\rho}(G_{\mathbb{Q}}) \subseteq \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ and consider the action of G on the symplectic vector space $V = A[\ell]$. Since G contains a transvection we may apply Theorem 3. To prove the theorem, it is sufficient to show that case (ii) of Theorem 3 does not arise. Suppose otherwise. Then we can write $V = \oplus_{i=1}^{h} V_i$ where V_i are non-singular symplectic subspaces of dimension $2m < 2d$, and there is some $\phi : G \to S_h$ with transitive image such that $\sigma(V_i) = V_{\phi(\sigma)(i)}$. Let $\pi = \phi \circ \overline{\rho}\colon G_{\mathbb{Q}} \to S_h$. Let $H = \mathrm{Ker}(\pi)$. Then $H = G_K$ for some number field $K/\mathbb{Q}$. Moreover, $\overline{\rho}|_{G_K}$ is reducible as the V_i are stable under the action of G_K. We shall show that the extension $K/\mathbb{Q}$ is unramified at the finite places, and thus K has discriminant ± 1. It then follows by a famous theorem of Hermite that $K = \mathbb{Q}$, showing that π is trivial and contradicting the fact that $\phi(G) = \pi(G_{\mathbb{Q}})$ is transitive.

First let $p \neq \ell$ be a prime. As A is semistable, I_p acts unipotently on V. Thus $\overline{\rho}(\sigma)$ has ℓ-power order for $\sigma \in I_p$. However, the order of $\overline{\rho}(\sigma)$ is divisible by the order of $\pi(\sigma)$ which in turn divides $h!$. As $h = 2d/2m \leq d < \ell$, we see that $\pi(\sigma) = 1$. Thus $K/\mathbb{Q}$ is unramified at p.

Next, consider $\sigma \in I_\ell^w$, the wild subgroup of I_ℓ. As I_ℓ^w is a pro-ℓ group, $\overline{\rho}(\sigma)$ has ℓ-power order, and we see that $\pi(\sigma) = 1$ as above. Finally, let $\sigma \in I_\ell$ be an element whose image in the tame inertia group $I_\ell^t = I_\ell/I_\ell^w$ is a topological generator. Reorder $V_1, \ldots, V_h$ so that $\sigma(V_i) = V_{i+1}$ for $i = 1, \ldots, r-1$ and $\sigma(V_r) = V_1$. Write $\overline{V} = V \otimes \overline{\mathbb{F}}_\ell$ and likewise define $\overline{V}_i$. Let $\overline{W} = \oplus_{i=1}^{r} \overline{V}_i$. It follows that $\overline{W}$ is stable under the action of I_ℓ. Let $\alpha_1 \in \overline{\mathbb{F}}_\ell$ be an eigenvalue for σ acting on $\overline{W}$. By Lemma 2.1, we know that $\alpha_2 = \zeta\alpha_1$ is also an eigenvalue for σ acting on $\overline{W}$, where $\zeta \in \overline{\mathbb{F}}_\ell$ is a primitive r-th root of unity (observe that this exists as $r \leq h \leq d < \ell$). By Raynaud's Theorem, there exist n_1, n_2 and characters $\varpi_j : I_\ell \to \mathbb{F}_{\ell^{n_j}}^{\times}$ such that $\alpha_j = \varpi_j(\sigma)$. As σ is a topological generator for the tame inertia and the characters ϖ_j are surjective, we see that α_1 and α_2 have orders $\ell^{n_1} - 1$, $\ell^{n_2} - 1$ respectively. Then $\zeta = \alpha_2/\alpha_1$ has order divisible by

$$(\ell^{n_1} - 1)(\ell^{n_2} - 1)/\gcd\left(\ell^{n_1} - 1, \ell^{n_2} - 1\right)^2 .$$

Suppose first that $n_1 \neq n_2$. Without loss of generality $n_1 < n_2$. Then $\gcd(\ell^{n_1} - 1, \ell^{n_2} - 1) \leq \ell^{n_1} - 1$. Thus

$$\frac{(\ell^{n_1} - 1)(\ell^{n_2} - 1)}{\gcd(\ell^{n_1} - 1, \ell^{n_2} - 1)^2} \geq \frac{(\ell^{n_2} - 1)}{(\ell^{n_1} - 1)} = \ell^{n_2 - n_1} + \frac{(\ell^{n_2 - n_1} - 1)}{(\ell^{n_1} - 1)} > \ell.$$

This contradicts the fact that the order of ζ is $r < \ell$. Thus $n_1 = n_2 = n$ (say). Now from Raynaud's Theorem, we know that

$$\varpi_1 = \psi_n^{a_0+a_1\ell+\cdots+a_{n-1}\ell^{n-1}}, \qquad \varpi_2 = \psi_n^{b_0+b_1\ell+\cdots+b_{n-1}\ell^{n-1}},$$

where $\psi_n : I_\ell \to \mathbb{F}_{\ell^n}^\times$ is a fundamental character of level n, and $0 \le a_i,\ b_i \le 1$. Since $\psi_n(\sigma)$ has order $\ell^n - 1$ and $\zeta = \varpi_2(\sigma)/\varpi_1(\sigma)$ has order r, we see that

$$r\sum_{i=0}^{n-1}(a_i - b_i)\ell^i \equiv 0 \pmod{\ell^n - 1}.$$

However $-1 \le a_i - b_i \le 1$ and so

$$\left| r\sum_{i=0}^{n-1}(a_i - b_i)\ell^i \right| \le r \cdot (\ell^n - 1)/(\ell - 1).$$

Since $r \le d \le \ell - 2$, we see that $r\sum_{i=0}^{n-1}(a_i - b_i)\ell^i = 0$, and hence $a_i = b_i$ for $i = 0, \ldots, n-1$. It follows that ζ has order 1. Since ζ is a primitive r-th root of unity, we have that $r = 1$. From the definition of r, we have that $\sigma(V_1) = V_1$. Similarly, $\sigma(V_j) = V_j$ for $j = 2, \ldots, h$. Hence $\pi(\sigma) = 1$. As we have shown that $\pi\left(I_\ell^w\right) = 1$, and as σ is a topological generator for the tame inertia, we have that $\pi(I_\ell) = 1$, showing that $K/\mathbb{Q}$ is unramified at ℓ. This completes the proof. □

3 Surjectivity for semistable principally polarized abelian threefolds

We now let $A/\mathbb{Q}$ be a principally polarized abelian threefold. We shall make the following assumptions henceforth:

(a) A is semistable;
(b) There is a prime q such that the special fibre of the Néron model for A at q has toric dimension 1.

Let S be the set of primes q satisfying (b). For $q \in S$, write Φ_q for the group of connected components of the special fibre of the Néron model of A at q. We shall suppose that

(c) $\ell \ge 5$;
(d) ℓ does not divide $\gcd(\{q \cdot \#\Phi_q : q \in S\})$.

Thus ([5], Section 2) the image of $\overline{\rho}_{A,\ell}$ contains a transvection. It follows from Theorem 2 that $\overline{\rho}_{A,\ell}$ is either reducible or surjective. In this section we explain a practical method which should in most cases produce a small integer B (depending on A) such that for $\ell \nmid B$, the representation $\overline{\rho}_{A,\ell}$ is irreducible and hence surjective.

3.1 Determinants of Jordan–Hölder factors

As before $\chi : G_\mathbb{Q} \to \mathbb{F}_\ell^\times$ denotes the mod ℓ cyclotomic character. We will study the Jordan–Hölder factors W of the $G_\mathbb{Q}$-module $A[\ell]$. By the determinant of such a W we mean the determinant of the induced representation $G_\mathbb{Q} \to \mathrm{GL}(W)$.

Lemma 3.1. *Any Jordan–Hölder factor W of the $G_\mathbb{Q}$-module $A[\ell]$ has determinant χ^r for some $0 \le r \le \dim(W)$.*

Proof. Let W be such a Jordan–Hölder factor, and let $\psi : G_\mathbb{Q} \to \mathbb{F}_\ell^\times$ be its determinant. As J is semistable, for primes $p \ne \ell$, the inertia subgroup $I_p \subset G_\mathbb{Q}$ acts unipotently on

W and so $\psi|_{I_p} = 1$. Moreover, by considering the Jordan–Hölder factors of W as an I_ℓ-module, it follows from Raynaud's Theorem that $\psi|_{I_\ell} = \chi^r|_{I_\ell}$ for some $0 \leq r \leq \dim(W)$. Thus the character $\psi\chi^{-r}$ is unramified at all the finite places. As the narrow class number of $\mathbb{Q}$ is 1, we see that $\psi\chi^{-r} = 1$ proving the lemma. □

3.2 Weil polynomials

For a prime $p \neq \ell$ of good reduction for A, we shall henceforth write

$$P_p(x) = x^6 + \alpha_p x^5 + \beta_p x^4 + \gamma_p x^3 + p\beta_p x^2 + p^2\alpha_p + p^3 \in \mathbb{Z}[x] \tag{2}$$

for the characteristic polynomial of Frobenius $\sigma_p \in G_\mathbb{Q}$ at p acting on the Tate module $T_\ell(A)$ (also known as the Weil polynomial of A mod p). The polynomial P_p is independent of ℓ. It follows from (2) that the roots in $\overline{\mathbb{F}}_\ell$ have the form $u, v, w, p/u, p/v, p/w$.

Lemma 3.2. *If P_p has a real root then $(x^2 - p)^2$ is a factor of P_p.*

Proof. By Weil, the complex roots have the form $\omega_1, \omega_2, \omega_3, \overline{\omega}_1, \overline{\omega}_2, \overline{\omega}_3$ where $|\omega_i| = \sqrt{p}$ and $\overline{\omega}$ denotes the complex conjugate of ω. Suppose ω_1 is real. Then $\omega_1 = \overline{\omega}_1$ and thus $(x - \omega_1)(x - \overline{\omega}_1) = (x - \omega_1)^2$ is a factor of P_p. Moreover, $\omega_1 = \pm\sqrt{p}$. The lemma follows as $P_p \in \mathbb{Z}[x]$. □

3.3 1-dimensional Jordan–Hölder factors

Let T be a non-empty set of primes of good reduction for A. Let

$$B_1(T) = \gcd(\{p \cdot \#A(\mathbb{F}_p) \ : \ p \in T\}). \tag{3}$$

Lemma 3.3. *Suppose $\ell \nmid B_1(T)$. The $G_\mathbb{Q}$-module $A[\ell]$ does not have any 1-dimensional or 5-dimensional Jordan–Hölder factors.*

Proof. As $\dim(A[\ell]) = 6$, if $A[\ell]$ has a 5-dimensional Jordan–Hölder factor then it has a 1-dimensional Jordan–Hölder factor. Suppose W is a 1-dimensional Jordan–Hölder factor of $A[\ell]$. Then the action of $G_\mathbb{Q}$ on W is given by a character $\psi : G_\mathbb{Q} \to \mathbb{F}_\ell^\times$. It follows from Lemma 3.1 that $\psi = 1$ or χ.

Let p be a prime of good reduction for A, and suppose $\ell \neq p$.

Thus P_p has root $\overline{1}$ or $\chi(\sigma_p) = \overline{p} \in \mathbb{F}_\ell$. Since the roots of P_p have the form $u, v, w, p/u, p/v, p/w$, we know in either case that $\overline{1}$ is a root, and so

$$\#A(\mathbb{F}_p) = P_p(1) \equiv 0 \pmod{\ell}.$$

Thus if p is a prime of good reduction for A, then ℓ divides $p \cdot \#A(\mathbb{F}_p)$. This proves the lemma. □

Since $\#A(\mathbb{F}_p) > 0$, we have $B_1(T) \neq 0$, and so we can always rule out 1-dimensional and 5-dimensional factors for large ℓ.

3.4 2-dimensional Jordan–Hölder factors

Lemma 3.4. *Suppose the $G_\mathbb{Q}$-module $A[\ell]$ does not have any 1-dimensional Jordan–Hölder factors, but has either a 2-dimensional or 4-dimensional irreducible subspace U. Then $A[\ell]$ has a 2-dimensional Jordan–Hölder factor W with determinant χ.*

Proof. Suppose $\dim(U) = 2$. If the restriction of the Weil pairing to U is non-degenerate then $\det(U) = \chi$ and we can take $W = U$. Thus we may suppose that the restriction of the Weil pairing to U is degenerate. Thus $U \cap U^\perp \neq 0$, where

$$U^\perp = \{v \in A[\ell] \,:\, \langle v, u\rangle = 0 \text{ for all } u \in U\}\,.$$

The Galois invariance of the Weil-pairing implies that $U^\perp$ is a $G_{\mathbb{Q}}$-submodule of $A[\ell]$. Since U is irreducible and $U \cap U^\perp \neq 0$ we have that $U \subseteq U^\perp$. However $U^\perp$ is 4-dimensional. Thus each of the 2-dimensional quotients in the sequence $0 \subset U \subset U^\perp \subset A[\ell]$ is 2-dimensional, must be irreducible (as $A[\ell]$ does not have 1-dimensional factors) and has determinant 1 or χ or χ^2 by Lemma 3.1. Since $\det(A[\ell]) = \chi^3$ we see that one the three quotients must have determinant χ. This completes the proof for the case $\dim(U) = 2$.

Now suppose that $\dim(U) = 4$. If the restriction of the Weil pairing to U is degenerate, then $U \subseteq U^\perp$ as before; this is impossible as $\dim(U^\perp) = 2$. It follows that the restriction of the Weil pairing to U is non-degenerate and so $\det(U) = \chi^2$. As $\det(A[\ell]) = \chi^3$, we have that $A[\ell]/U$ is an irreducible 2-dimensional $G_{\mathbb{Q}}$-module with determinant χ. This completes the proof. □

Let N be the conductor of A. Let W be a 2-dimensional Jordan–Hölder factor of $A[\ell]$ with determinant χ. The representation

$$\tau : G_{\mathbb{Q}} \to \mathrm{GL}(W) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$$

is odd (as the determinant is χ), irreducible (as W is a Jordan–Hölder factor) and 2-dimensional. By Serre's modularity conjecture, now a theorem of Khare and Wintenberger ([6], Theorem 1.2), this representation arises from a newform f of level $M \mid N$ and weight 2. Let $\mathcal{O}_f$ be the ring of integers of the number field generated by the Hecke eigenvalues of f. Then there is a prime $\lambda \mid \ell$ of $\mathcal{O}_f$ such that for all primes $p \nmid \ell N$,

$$\mathrm{tr}(\tau(\sigma_p)) \equiv c_p(f) \pmod{\lambda}$$

where $\sigma_p \in G_{\mathbb{Q}}$ is a Frobenius element at p and $c_p(f)$ is the p-th Hecke eigenvalue of f. Hence $x^2 - c_p(f)\,x + p$ is congruent modulo λ to the characteristic polynomial of $\tau(\sigma_p)$. As W is a Jordan–Hölder factor of $A[\ell]$ we see that $x^2 - c_p(f)\,x + p$ is a factor modulo λ of P_p. Now let $H_{M,p}$ be the p-th Hecke polynomial for the new subspace $S_2^{\mathrm{new}}(M)$ of cusp forms of weight 2 and level M. This has the form $H_{M,p} = \prod(x - c_p(g))$ where g runs through the newforms of weight 2 and level M. We shall write

$$H'_{M,p}(x) = x^d H_{M,p}(x + p/x) \in \mathbb{Z}[x]\,, \qquad d = \deg(H_{M,p}) = \dim(S_2^{\mathrm{new}}(M))\,.$$

It follows that $x^2 - c_p(f)\,x + p$ divides $H'_{M,p}$. Let

$$R(M,p) = \mathrm{Res}\left(P_p, H'_{M,p}\right) \in \mathbb{Z}, \tag{4}$$

where Res denotes resultant. It is immediate that $\lambda \mid R(M,p)$. As $R(M,p)$ is a rational integer, we have $\ell \mid R(M,p)$. If $R(M,p) \neq 0$ then we obtain a bound on ℓ. We can of course work directly with $\mathrm{Res}(P_p, x^2 - c_p(f)\,x + p)$, which produces an integer in $\mathcal{O}_f$ divisible by λ, and if this algebraic integer is non-zero it would lead us to a bound on ℓ. However, in general it is much easier and faster to write down the Hecke polynomials $H_{M,p}$ than it is to compute the individual eigenforms f.

The integers $R(M,p)$ can be very large (see the example below). Given a non-empty set T of rational primes p of good reduction for A, we shall let

$$R(M,T) = \gcd(\{p \cdot R(M,p) \ : \ p \in T\}).$$

In practice, we have found that for a suitable choice of T, the value $R(M,T)$ is fairly small. Now let

$$B_2'(T) = \operatorname{lcm}(R(M,T))$$

where M runs through the divisors of N such that $\dim(S_2^{\text{new}}(M)) \neq 0$, and let

$$B_2(T) = \operatorname{lcm}(B_1(T), B_2'(T)),$$

where $B_1(T)$ is given by (3).

Lemma 3.5. *Let T be a non-empty set of rational primes of good reduction for A, and suppose $\ell \nmid B_2(T)$. Then $A[\ell]$ does not have 1-dimensional Jordan–Hölder factors, and does not have irreducible 2- or 4-dimensional subspaces.*

Proof. By Lemmas 3.3 and 3.4 it is enough to rule out the existence of a 2-dimensional Jordan–Hölder factor with character χ. This follows from the above discussion. □

Of course we fail to bound ℓ in the above lemma if $R(M,p) = 0$ for all primes p of good reduction. Here are two situations where this can happen:

- Suppose A is isogenous over $\mathbb{Q}$ to $E \times A'$ where E is an elliptic curve and A' an abelian surface. If we take $M \mid N$ to be the conductor of the elliptic curve, and f to be the newform associated to E by modularity, then $x^2 - c_p(f)x + p$ is a factor of $P_p(x)$ in $\mathbb{Z}[x]$. Thus the resultant $R(M,p) = 0$ for all $p \nmid N$.
- Suppose the abelian threefold A is of GL_2-type. It is therefore modular by Khare and Wintenberger [6], and if we let f be the corresponding eigenform, then again $x^2 - c_p(f)x + p$ is a factor of $P_p(x)$ in $\mathcal{O}_f[x]$, and so the resultant $R(M,p) = 0$ for all $p \nmid N$.

Note that in both these situations $\operatorname{End}_{\overline{\mathbb{Q}}}(A) \neq \mathbb{Z}$. We expect, but are unable to prove, that if $\operatorname{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$ then there will be primes p such that $R(M,p) \neq 0$.

3.5 3-dimensional Jordan–Hölder factors

Lemma 3.6. *Suppose $A[\ell]$ has Jordan–Hölder filtration $0 \subset U \subset A[\ell]$ where both U and $A[\ell]/U$ are irreducible and 3-dimensional. Moreover, let u_1, u_2, u_3 be a basis for U, and let*

$$G_{\mathbb{Q}} \to \mathrm{GL}_3(\mathbb{F}_\ell), \qquad \sigma \mapsto M(\sigma)$$

give the action of $G_{\mathbb{Q}}$ on U with respect to this basis. Then we can extend u_1, u_2, u_3 to a symplectic basis u_1, u_2, u_3, w_1, w_2, w_3 for $A[\ell]$ so that the action of $G_{\mathbb{Q}}$ on $A[\ell]$ with respect to this basis is given by

$$G_{\mathbb{Q}} \to \mathrm{GSp}_6(\mathbb{F}_\ell), \qquad \sigma \mapsto \left(\begin{array}{c|c} M(\sigma) & * \\ \hline \mathbf{0} & \chi(\sigma)(M(\sigma)^t)^{-1} \end{array}\right).$$

Proof. Any bilinear alternating pairing on an odd dimensional space (in characteristic $\neq 2$) must be degenerate. We thus deduce that $U \subseteq U^{\perp}$ as in the proof of Lemma 3.4. As both spaces have dimension 3, we have $U = U^{\perp}$. Let u_1, u_2, u_3 be a basis for U. Then $\langle u_i, u_j \rangle = 0$. Extend this to a symplectic basis $u_1, u_2, u_3, w_1, w_2, w_3$ for $A[\ell]$: meaning that in addition to $\langle u_i, u_j \rangle = 0$ the basis satisfies $\langle w_i, w_j \rangle = 0$, and $\langle u_i, w_j \rangle = \delta_{i,j}$ where $\delta_{i,j}$ is the Kronecker delta. The lemma follows from the identity $\langle u_i, \sigma w_j \rangle = \chi(\sigma)\langle \sigma^{-1} u_i, w_j \rangle$ for $\sigma \in G_{\mathbb{Q}}$. □

Now let U be as in Lemma 3.6. By Lemma 3.1, we have that $\det(U) = \chi^r$ and $\det(A[\ell]/U) = \chi^s$ where $0 \leq r, s \leq 3$. Moreover, as $\det(A[\ell]) = \chi^3$ we have that $r+s = 3$.

Lemma 3.7. *Let p be a prime of good reduction for A. For ease write α, β and γ for the coefficients α_p, β_p, γ_p in (2). Suppose $p + 1 \neq \alpha$ (this is certainly true for $p \geq 36$ as $|\alpha| \leq 6\sqrt{p}$). Let*

$$\delta = \frac{-p^2\alpha + p^2 + p\alpha^2 - p\alpha - p\beta + p - \beta + \gamma}{(p-1)(p+1-\alpha)} \in \mathbb{Q}, \qquad \epsilon = \delta + \alpha \in \mathbb{Q}. \tag{5}$$

Let

$$g(x) = \left(x^3 + \epsilon x^2 + \delta x - p\right)\left(x^3 - \delta x^2 - p\epsilon x - p^2\right) \in \mathbb{Q}[x]. \tag{6}$$

Write k for the greatest common divisor of the numerators of the coefficients in $P_p - g$. Let

$$K_p = p(p-1)(p+1-\alpha)k.$$

Then $K_p \neq 0$. Moreover, if $\ell \nmid K_p$ then $A[\ell]$ does not have a Jordan–Hölder filtration as in Lemma 3.6 with $\det(U) = \chi$ or χ^2.

Lemma 3.8. *Let p be a prime of good reduction for A. Write α, β and γ for the coefficients α_p, β_p, γ_p in (2). Suppose $p^3 + 1 \neq p\alpha$ (this is true for $p \geq 5$ as $|\alpha| \leq 6\sqrt{p}$). Let*

$$\delta' = \frac{-p^5\alpha + p^4 + p^3\alpha^2 - p^3\beta - p^2\alpha + p\gamma + p - \beta}{(p^3-1)(p^3+1-p\alpha)} \in \mathbb{Q}, \qquad \epsilon' = p\delta' + \alpha \in \mathbb{Q}. \tag{7}$$

Let

$$g'(x) = \left(x^3 + \epsilon' x^2 + \delta' x - 1\right)\left(x^3 - p\delta' x^2 - p^2\epsilon' x - p^3\right) \in \mathbb{Q}[x]. \tag{8}$$

Write k' for the greatest common divisor of the numerators of the coefficients in $P_p - g'$. Let

$$K'_p = p\left(p^3 - 1\right)\left(p^3 + 1 - p\alpha\right)k'.$$

Then $K'_p \neq 0$. Moreover, if $\ell \nmid K'_p$ then $A[\ell]$ does not have a Jordan–Hölder filtration as in Lemma 3.6 with $\det(U) = 1$ or χ^3.

Proof of Lemma 3.7 and 3.8. For now let p be a prime of good reduction for A, and suppose that $\ell \neq p$. Suppose $A[\ell]$ has a Jordan–Hölder filtration $0 \subset U \subset A[\ell]$ where U and $A[\ell]/U$ are 3-dimensional (i.e. as in Lemma 3.6). Then $\det(U) = \chi^r$ with $0 \leq r \leq 3$. Let $\sigma_p \in G_{\mathbb{Q}}$ denote a Frobenius element at p. Let $M = M(\sigma_p)$ as in Lemma 3.6. Then $\det(M) = \overline{p}^r \in \mathbb{F}_\ell$. Moreover, from the lemma,

$$P_p(x) \equiv \det(xI - M)\det\left(xI - pM^{-1}\right) \pmod{\ell}.$$

Write

$$\det(xI - M) \equiv x^3 + ux^2 + vx - p^r \pmod{\ell}.$$

Then

$$\begin{aligned}\det\left(xI - pM^{-1}\right) &= -p^{-r} \cdot x^3 \cdot \det\left(px^{-1}I - M\right) \\ &\equiv x^3 - p^{1-r}vx^2 - p^{2-r}ux - p^{3-r} \pmod{\ell}.\end{aligned}$$

Let

$$a = \begin{cases} u & \text{if } r = 0 \text{ or } 1 \\ -p^{-1}v & \text{if } r = 2 \\ -p^{-2}v & \text{if } r = 3 \end{cases} \qquad b = \begin{cases} v & \text{if } r = 0 \text{ or } 1 \\ -u & \text{if } r = 2 \\ -p^{-1}u & \text{if } r = 3. \end{cases}$$

If $r = 1$ or 2 then

$$P_p(x) \equiv \left(x^3 + ax^2 + bx - p\right)\left(x^3 - bx^2 - pax - p^2\right) \pmod{\ell}. \tag{9}$$

If $r = 0$ or 3 then

$$P_p(x) \equiv \left(x^3 + ax^2 + bx - 1\right)\left(x^3 - pbx^2 - p^2ax - p^3\right) \pmod{\ell}. \tag{10}$$

We now suppose that $\ell \nmid K_p$ and prove Lemma 3.7 which corresponds to $r = 1$ or 2. We thus suppose that (9) holds. Comparing the coefficients of x^5 in (9) we have that $a \equiv b + \alpha \pmod{\ell}$. Substituting this into (9) and comparing the coefficients of x^4 and x^3 we obtain

$$\begin{aligned} b^2 + (p + \alpha - 1) \cdot b + (p\alpha + \beta) &\equiv 0 \pmod{\ell} \\ (p+1) \cdot b^2 + 2p\alpha \cdot b + \left(p^2 + p\alpha^2 + p + \gamma\right) &\equiv 0 \pmod{\ell}. \end{aligned}$$

Eliminating b^2 we obtain the following congruence which is linear in b:

$$-(p-1)(p+1-\alpha) \cdot b + \left(-p^2\alpha + p^2 + p\alpha^2 - p\alpha - p\beta + p - \beta + \gamma\right) \equiv 0 \pmod{\ell}.$$

As $\ell \nmid K_p$ we have $\ell \nmid (p-1)(p+1-\alpha)$, and so we can solve for $b \bmod \ell$. It follows that $b \equiv \delta$ and $a \equiv b + \alpha \equiv \epsilon \pmod{\ell}$ where δ and ϵ are given by (5). Substituting into (9), we see that $P_p \equiv g \pmod{\ell}$ where g is given by (6). Thus ℓ divides the greatest common divisor of the numerators of the coefficients of $P_p - g$ showing that $\ell \mid k$ (in the notation of Lemma 3.7). As $k \mid K_p$ and $\ell \nmid K_p$ we obtain a contradiction. Thus if $\ell \nmid K_p$ then $A[\ell]$ does not have a Jordan–Hölder filtration as in Lemma 3.6 with $\det(U) = \chi$ or χ^2.

We need to show that $K_p \neq 0$. We are supposing that $p + 1 \neq \alpha$ thus we need to show that $P_p \neq g$. Suppose $P_p = g$. As g is the product of two cubic polynomials, it follows that P_p has at least two real roots. By Lemma 3.2, we see that $(x^2 - p)^2 \mid P_p$. It follows that $P_p = g$ must have two rational roots. Since all the roots have absolute value $\sqrt{p}$, this is a contradiction. We deduce that $K_p \neq 0$ as required. This completes the proof of Lemma 3.7. The proof of Lemma 3.8 is practically identical. □

3.6 Summary

The following theorem summarizes Section 3.

Theorem 5. *Let A and ℓ satisfy conditions (a)–(d) at the beginning of Section 3. Let T be a non-empty set of primes of good reduction for A. Let*

$$B_3(T) = \gcd\left(\left\{K_p \,:\, p \in T\right\}\right), \qquad B_4(T) = \gcd\left(\left\{K'_p \,:\, p \in T\right\}\right),$$

where K_p and K'_p are defined in Lemmas 3.7 and 3.8. Let

$$B(T) = \operatorname{lcm}(B_2(T), B_3(T), B_4(T))$$

where $B_2(T)$ is as in Lemma 3.5. If $\ell \nmid B(T)$ then $\overline{\rho}_{A,\ell}$ is surjective.

Proof. By Theorem 2 we know that $\overline{\rho}_{A,\ell}$ is either reducible or surjective. Lemmas 3.5, 3.7 and 3.8 ensure that $\overline{\rho}_{A,\ell}$ cannot be reducible. Hence it must be surjective. □

4 Proof of Corollary 1.1

We implemented the method described in Section 3 in `Magma` [3]. The model given in (1) for the curve C has good reduction at 2. Let J be the Jacobian of C. This has conductor $N = 8907 = 3 \times 2969$ (the algorithm used by `Magma` for computing the conductor is described in (Dokchitser T., Dokchitser V., Maistret C. and Morgan A.: *Arithmetic of hyperelliptic curves over local fields*, in preparation). As N is squarefree, the Jacobian J is semistable. Completing the square in (1) we see that the curve C has the following 'simplified' Weierstrass model.

$$y^2 = x^8 + 2x^7 + 5x^6 + 6x^5 + 4x^4 + 2x^3 + x^2 + 2x + 1.$$

Denote the polynomial on the right-hand side by f. Then

$$f \equiv (x+1)(x+2)^2\left(x^2+x+2\right)\left(x^3+2x^2+2x+2\right) \pmod 3$$

and

$$f \equiv (x+1)(x+340)(x+983)^2\left(x^2+x+1\right)\left(x^2+663x+1350\right) \pmod{2969}.$$

Here the non-linear factors in both factorizations are irreducible. As f has precisely one double root in $\overline{\mathbb{F}}_3$ and one double root in $\overline{\mathbb{F}}_{2969}$ with all other roots simple, we see that the Néron models for J at 3 and 2969 have special fibres with toric dimension 1. We found that $\#\Phi_3 = \#\Phi_{2969} = 1$. Thus the image of $\overline{\rho}_{J,\ell}$ contains a transvection for all $\ell \geq 3$.

We now suppose $\ell \geq 5$. By Theorem 2 we know that $\overline{\rho}_{J,\ell}$ is either reducible or surjective. In the notation of Section 3, we take our chosen set of primes of good reduction to be $T = \{2, 5, 7\}$. We note that

$$\#J(\mathbb{F}_2) = 2^5, \qquad \#J(\mathbb{F}_5) = 2^7, \qquad \#J(\mathbb{F}_7) = 2^6 \times 7.$$

It follows from Lemma 3.3 that $J[\ell]$ does not have 1- or 5-dimensional Jordan–Hölder factors. Next we consider the existence of 2- or 4-dimensional irreducible subspaces. The possible values $M \mid N$ such that $S_2^{\text{new}}(M) \neq 0$ are $M = 2969$ and $M = 8907$, where the dimensions are 247 and 495 respectively. Unsurprisingly, the resultants $R(M, p)$ (defined in (4)) are too large to reproduce here. For example, we indicate that $R(8907, 7) \sim 1.63 \times 10^{2344}$. However,

$$R(M,T) = \gcd\left(2 \cdot R(M,2),\ 5 \cdot R(M,5),\ 7 \cdot R(M,7)\right) = \begin{cases} 2^4 & M = 2969, \\ 2^{22} & M = 8907. \end{cases}$$

It follows from Lemma 3.5 that $J[\ell]$ does not have 2- or 4-dimensional irreducible subspaces. It remains to eliminate the possibility of a Jordan–Hölder filtration $0 \subset U \subset J[\ell]$ where both U and $J[\ell]/U$ are 3-dimensional. In the notation of Lemma 3.7,

$$K_2 = 14, \qquad K_5 = 6900, \qquad K_7 = 83202.$$

Then $\gcd(K_2, K_5, K_7) = 2$. Lemma 3.7 eliminates the case where $\det(U) = \chi$ or χ^2. Moreover,

$$K_2' = 154490, \qquad K_5' = 15531373270380, \qquad K_7' = 10908656905042386.$$

Then $\gcd\left(K_2', K_3', K_7'\right) = 2$. Lemma 3.8 eliminates the case where $\det(U) = 1$ or χ^3. It follows that $\overline{\rho}_{J,\ell}$ is irreducible and hence surjective for all $\ell \geq 5$.

It remains to show that $\overline{\rho}_{J,3}$ is surjective. Denote $\overline{\rho} = \overline{\rho}_{J,3}$. Write $G = \overline{\rho}(G_{\mathbb{Q}})$. For a prime p of good reduction, let $\sigma_p \in G_{\mathbb{Q}}$ denote a Frobenius element at p and $\overline{P}_p \in \mathbb{F}_3[t]$ be the characteristic polynomial of σ_p acting on $J[3]$. Let N_p be the multiplicative order of the image of t in the algebra $\mathbb{F}_3[t]/\overline{P}_p$. It is immediate that N_p divides the order of $\overline{\rho}(\sigma_p)$ and hence divides the order of G. We computed

$$N_2 = 2^3 \times 5, \qquad N_5 = 2 \times 13, \qquad N_{19} = 7, \qquad N_{37} = 2 \times 3^2.$$

Thus the order of G is divisible by $2^3 \times 3^2 \times 5 \times 7 \times 13$. We checked that the only subgroups of $\mathrm{GSp}_6(\mathbb{F}_3)$ with order divisible by this are $\mathrm{Sp}_6(\mathbb{F}_3)$ and $\mathrm{GSp}_6(\mathbb{F}_3)$. As the mod 3 cyclotomic character is surjective on $G_{\mathbb{Q}}$, we have that $G = \mathrm{GSp}_6(\mathbb{F}_3)$. This completes the proof of the corollary.

Acknowledgements
The first-named and third-named authors are supported by EPSRC Programme Grant 'LMF: L-Functions and Modular Forms' EP/K034383/1.

Received: 10 August 2015 Accepted: 23 November 2015
Published online: 15 February 2016

References

1. Arias-de Reyna, S, Armana, C, Karemaker, V, Rebolledo, M, Thomas, L, Vila, N: Galois representations and galois groups over $\mathbb{Q}$ (2014). ArXiv e-prints
2. Arias-de-Reyna, S, Dieulefait, L, Wiese, G: Classification of subgroups of symplectic groups over finite fields containing a transvection (2014). ArXiv e-prints
3. Bosma, W, Cannon, J, Playoust, C: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265 (1997). Computational algebra and number theory (London, 1993)
4. Dieulefait, LV: Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathbf{End}(A) = \mathbb{Z}$. Experiment. Math. **11**(4), 503–512(2003) (2002)
5. Hall, C: An open-image theorem for a general class of abelian varieties. Bull. Lond. Math. Soc. **43**(4), 703–711 (2011). With an appendix by Emmanuel Kowalski
6. Khare, C, Wintenberger, J-P: Serre's modularity conjecture. I. Invent. Math. **178**(3), 485–504 (2009)
7. Lombardo, D: Explicit open image theorems for some abelian varieties with trivial endomorphism ring (2015). ArXiv e-prints
8. Mazur, B: Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. **44**(2), 129–162 (1978)
9. Mumford, D: A note of Shimura's paper "Discontinuous groups and abelian varieties". Math. Ann. **181**(4), 345–351 (1969)
10. Raynaud, M: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. France. **102**, 241–280 (1974)
11. Serre, J-P: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
12. Serre, J-P: Oeuvres/Collected papers. IV. 1985–1998. Springer Collected Works in Mathematics. Springer, Heidelberg (2013). Reprint of the 2000 edition [MR1730973]
13. Zywina, D: An explicit Jacobian of dimension 3 with maximal Galois action (2015). ArXiv e-prints